



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/081,061	02/20/2002	Kunihiko Miyazaki	16869S-043400US	5417

20350 7590 08/17/2005

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER

ELMORE, JOHN E

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 08/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/081,061

Applicant(s)

MIYAZAKI ET AL.

Examiner

John Elmore

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on 20 February 2002.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-19 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 20 February 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 2/20/02, 6/14/02.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED INFORMATION

1. Claims 1-19 have been examined.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. **Claims 1-4, 6, 7, 14 and 15 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Boebert et al. (US 4,713,753), hereafter Boebert, in view of McCollum et al. (US 6,006,228), hereafter McCollum.

Regarding claim 1, Boebert discloses a computer system having an input/output processing unit for executing a file access, an access execution unit for requesting file access to the input/output processing unit in response to a user instruction, and an access control unit for performing access control when the file access is executed, wherein:

said access control unit (part of secure computer 33 and memory 22) comprises:

a storage unit protected from the access execution unit (memory 22 protected by memory address apparatus 336 in secure processor 33 via access rights 622; col. 10, lines 62-67);

a file list stored on said storage unit describing security levels of files (data objects characteristics table 333; col. 9, lines 65-67);

an access control processing unit for judging whether the file access is legal in accordance with said file list, said user list, an access type (access mode) of file access, information identifying a file, and information identifying a user (secure computer 33; Fig. 3 and 8; col. 7, line 52 – col. 8, line 7; col. 9, lines 21-26; col. 10, lines 28-39); and

an access monitor unit (user entity identification apparatus 31, program working set table 334 and tag code recognition apparatus 336a) which:

sends, when the input/output processing unit executes access, the access type (access mode), the information identifying the file, the information identifying the user to said access control processing unit (apparatus 31 sends user information to current security content register 331 as well as sends file identification and access mode to ordinary data object processing unit 32; col. 7, lines 56-62);

receives a validity judgment (access right 622) as a result of the file access from said access control processing unit (program working set table 334 receives access right 622 from security policy unit 332 via distinguished data object processing unit 335; col. 10, lines 3-5 and 28-67; col. 11, lines 3-11); and

if the file access is legal, makes the input/output processing unit execute the file access, whereas the file access is illegal, inhibits the file access (memory address apparatus 336 executes the file access only where legally permitted by access right 622; col. 9, lines 21-26).

But Boebert does not explicitly explain that said access control unit comprises a user list stored on said storage unit describing clearances of users.

However, Boebert teaches a list of authorized users for the purpose of determining a validity judgment (access right 622) for accessing a file (col. 10, lines 34-39) as well as the maintenance of user information describing security clearance levels by the current security context register 331; col. 9, line 67 – col. 10, line 3). One of ordinary skill in the art would recognize that the authorized list would include information describing security clearance levels because authorization is determined by comparing the clearance level of the requested file to that of the requesting user. Further, McCollum teaches system for securing access to files by employing a user list (User Table 100) describing security clearance levels for the purpose of keeping track of users and their security privileges (Fig. 2; col. 2, lines 62-67).

Therefore, it would be obvious to one of ordinary skill to modify the system of Boebert with the teaching of McCollum to provide that said access control unit comprises a user list stored on said storage unit describing clearances of users. One would be motivated to do so in order to facilitate security policy monitoring by keeping track of users and their security privileges.

Regarding claim 2, the modified system of Boebert and McCollum is relied upon as applied to claim 1, and Boebert and McCollum further teach an exclusive control unit for protecting a storage area of said storage unit to be used by said access control processing unit from the access execution unit (Boebert: secure processor 33 has

Art Unit: 2134

exclusive control for protection of memory 22; Fig. 2; col. 3, line 62 – col. 4, line 3; col. 8, lines 7-10).

Regarding claim 3, the modified system of Boebert and McCollum is relied upon as applied to claim 2, and Boebert and McCollum further teach a user setting/managing unit for setting and managing said user list (McCollum: security database; col. 2, lines 33-38; col. 3, lines 41-52).

Regarding claim 4, the modified system of Boebert and McCollum is relied upon as applied to claim 3, but Boebert and McCollum do not explicitly explain that said user list setting/managing unit includes an authentication unit for authenticating a security administrator.

However, Boebert and McCollum teach that the secure processor 33 may be accessed, and data therein manipulated, only by a security administrator (Boebert: security officer; col. 8, lines 17-19) and that the user list resides within the domain of the secure processor 33 (Boebert: col. 10, lines 34-35). The Examiner takes official notice that one of ordinary skill in the art would recognize that an authentication unit for authentication of a security administrator is necessary for maintaining secure handling of the user list because access to the user list by persons other than a trusted security administrator exposes the list to tampering, which in turn jeopardizes the security of the files in memory 22. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to provide that said user list setting/managing unit includes an authentication unit for authenticating a security administrator for the

motivation of ensuring that only an authorized security administrator can modify the user list.

Regarding claim 6, the modified system of Boebert and McCollum is relied upon as applied to claim 1, and Boebert and McCollum further teach a file list setting/managing unit for setting and managing said file list (distinguished data object processing unit 335; col. 9, lines 65-67).

Regarding claim 7, the modified system of Boebert and McCollum is relied upon as applied to claim 6, but Boebert and McCollum do not explicitly explain that said file list setting/managing unit includes an authentication unit for authenticating a security administrator.

However, Boebert and McCollum teach that the secure processor 33 may be accessed, and data therein manipulated, only by a security administrator (Boebert: security officer; col. 8, lines 17-19) and that the file list (data object characteristics table 333) resides within the domain of the secure processor 33 (Boebert: Fig. 2). The Examiner takes official notice that one of ordinary skill in the art would recognize that an authentication unit for authentication of a security administrator is necessary for maintaining secure handling of the file list because access to the file list by persons other than a trusted security administrator exposes the list to tampering, which in turn jeopardizes the security of the files in memory 22. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to provide that said file list setting/managing unit includes an authentication unit for authenticating a security

administrator for the motivation of ensuring that only an authorized security administrator can modify the file list.

Regarding claim 14, the modified system of Boebert and McCollum is relied upon as applied to claim 1, and Boebert and McCollum further teach that the access control unit is realized by a software module (col. 8, lines 20-25). Therefore, for reasons applied above, such a claim also would have been obvious.

Regarding claim 15, the modified system of Boebert and McCollum is relied upon as applied to claim 1, and Boebert and McCollum further teach that the access control unit is realized by a hardware module (col. 8, lines 19-20; col. 13, lines 51-64). Therefore, for reasons applied above, such a claim also would have been obvious.

4. **Claims 5 and 8 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Boebert, in view of McCollum and further in view of Digital Equipment Corporation ("Security," March 1996), hereafter DEC.

Regarding claim 5, the modified system of Boebert and McCollum is relied upon as applied to claim 3, but Boebert and McCollum do not explicitly explain that security administrator is different from a system administrator who manages the access execution unit.

However, Boebert and McCollum teach that the administrator is a security officer (Boebert: col. 8, lines 17-19). And DEC teaches a computer system wherein a security administrator is different from a system administrator, who manages the access execution unit, for the purpose of enhancing security by providing checks and balances

via the separation of security-related tasks from other administrative tasks (pages 12-14, particularly sections 6.5.1.1 and 6.5.1.2).

Therefore, it would be obvious to one of ordinary skill to modify the modified system of Boebert and McCollum with the teaching of DEC to provide that the security administrator is different from the system administrator who manages the access execution unit. One would be motivated to do so in order to enhance security by providing checks and balances via the separation of security-related tasks from other administrative tasks, particularly where the file system is protected by a secure computer.

Regarding claim 8, this claim is rejected for the same reasons as provided above for claim 5.

5. **Claims 9-11 and 16-19 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Boebert, in view of McCollum, further in view of Scheidt et al. (US 6,754,820), hereafter Scheidt.

Regarding claim 9, the modified system of Boebert and McCollum is relied upon as applied to claim 1, but Boebert and McCollum do not explicitly explain an enciphering unit for enciphering a file if the file access for requesting to output a file to said storage unit is legal and a deciphering unit for deciphering the enciphered file if the file access for requesting to input the enciphered file from said storage unit is legal.

However, Boebert and McCollum teach an enciphering unit (encryption apparatus 337) and a deciphering unit (decryption apparatus 337) as part of the secure

computer system 33 (Boebert: Fig. 3). And Scheidt teaches an enciphering unit for enciphering a file if the file access for requesting to output a file to said storage unit is legal and a deciphering unit for deciphering the enciphered file if the file access for requesting to input the enciphered file from said storage unit is legal (col. 2, lines 14-24; col. 4, lines 8-13; col. 5, lines 10-27) for the purpose of enhancing security by using cryptography rather than software to provide access control for a computer file system (col. 2, lines 57-64).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the modified system of Boebert and McCollum with the teaching of Scheidt to provide an enciphering unit for enciphering a file if the file access for requesting to output a file to said storage unit is legal and a deciphering unit for deciphering the enciphered file if the file access for requesting to input the enciphered file from said storage unit is legal. One would be motivated to do so in order to enhance security by using cryptography rather than software to provide access control for a computer file system.

Regarding claim 10, the modified system of Boebert, McCollum and Scheidt is relied upon as applied to claim 9, but Boebert, McCollum and Scheidt do not explicitly explain an exclusive control unit that protects from the access execution unit a storage area in said storage unit storing at least one key information set to be used by said enciphering unit and said deciphering unit.

However, the Examiner takes official notice that one of ordinary skill would recognize that where the modified system of Boebert, McCollum and Scheidt maintains

exclusive control over the encrypted file system in memory 22, the system must also maintain exclusive control over at least one key information set to be used for enciphering and deciphering files in order to ensure the security of the file system, particularly where the cryptographic operations are integrated into the operating system of the secure computer 33. Therefore, it would be obvious to one of ordinary skill in the art to modify the modified system of Boebert, McCollum and Scheidt to provide for an exclusive control unit that protects from the access execution unit a storage area in said storage unit storing at least one key information set to be used by said enciphering unit and said deciphering unit for the motivation of enhancing security.

Regarding claim 11, the modified system of Boebert, McCollum and Scheidt is relied upon as applied to claim 9, but Boebert, McCollum and Scheidt do not explicitly explain that said enciphering unit and said deciphering unit use a plurality set of different key information and at least one cipher method for each security level written in said file list.

However, Scheidt further teaches an access control system wherein an enciphering unit and a deciphering unit use a plurality set of different key information and at least one cipher method for each security level written in said file list for the purpose of providing a more balanced security approach (different keys and different cryptographic algorithms are used for each security level in providing secure access to a user of protected information; col. 4, lines 33-57; col. 5, lines 10-27 and 38-50; col. 6, lines 34-37; col. 7, lines 15-32).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the modified system of Boebert, McCollum and Scheidt with the further teaching of Scheidt to provide that said enciphering unit and said deciphering unit use a plurality set of different key information and at least one cipher method for each security level written in said file list. One would be motivated to do so in order to provide a more balanced security approach to multiple-level access control.

Regarding claim 16, this is another system version of the claimed system above (claims 1 and 9). Therefore, for reasons applied above, such a claim also is obvious.

Regarding claim 17, the modified system of Boebert, McCollum and Scheidt is relied upon as applied to claim 16, but Boebert, McCollum and Scheidt do not explicitly explain that said cipher function processing unit includes an authentication unit for authenticating a user.

However, Boebert, McCollum and Scheidt teach that the users in the user list are authorized (). And Scheidt further teaches a means of authorizing users in a user list associated with a secure file system wherein a cipher function processing unit includes an authentication unit for authenticating a user for the purpose of establishing that a user's security level and other profile information are genuine (authentication unit authenticates user for inclusion in user list by verifying a digital signature; col. 7, lines 48-62).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the modified system of Boebert, McCollum and Scheidt with the further teaching of Scheidt to provide that said cipher function processing unit

Art Unit: 2134

includes an authentication unit for authenticating a user. One would be motivated to do so in order to establish that a user's security level and other profile information are genuine.

Regarding claim 18, the modified system of Boebert, McCollum and Scheidt is relied upon as applied to claim 16, but Boebert, McCollum and Scheidt do not explicitly explain that said cipher function processing unit is realized by a software module.

However, Boebert, McCollum and Scheidt further teach that the secure file system is realized by a software module (col. 8, lines 20-25). And it is widely known in the art that cryptographic processing is operable by a software module. The Examiner takes official notice that one of ordinary skill in the art would recognize that where the main components of the secure file system are implemented in a software module, the cryptographic processing would normally be operable by a software module. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to provide that cryptographic processing is operable by a software module for the motivation of maintaining efficiency and consistency of design.

Regarding claim 19, the modified system of Boebert, McCollum and Scheidt is relied upon as applied to claim 61, but Boebert, McCollum and Scheidt do not explicitly explain that said cipher function processing unit is realized by a software module.

However, Boebert, McCollum and Scheidt further teach that the secure file system is realized by a hardware module (col. 8, lines 19-20; col. 13, lines 51-64). And it is widely known in the art that cryptographic processing is operable by a software module. The Examiner takes official notice that one of ordinary skill in the art would

recognize that where the main components of the secure file system are implemented in a software module, the cryptographic processing would normally be operable by a software module. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to provide that cryptographic processing is operable by a hardware module for the motivation of maintaining efficiency and consistency of design

6. **Claims 12 and 13 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Boebert in view of McCollum, and further in view of Dryer et al. (US 2002/0099666), hereafter Dryer.

Regarding claim 12, the modified system of Boebert and McCollum is relied upon as applied to claim 1, but Boebert and McCollum do not explain an input/output monitor unit for monitoring that the input/output processing unit or said access monitor unit is not tampered or performs a predetermined operation, and instructing to inhibit an input/output of a file if the input/output processing unit or said access monitor unit is tampered or performs an operation different from the predetermined operation.

However, Dryer teaches a secure file access control system wherein an input/output monitor unit (file access monitor 134 and internal integrity checks 132) for monitoring that the secure computer system (Lockbox, which contains a secure file system) is not tampered, and instructing to inhibit operation of the secure computer if secure computer is tampered for the purpose of protecting the data within the secure computer from tampering and other unauthorized access (detection of tampering triggers alarm; para. 0012 and 0023) for the purpose of enhancing security, particularly

where a high degree of confidentiality is required (para. 0011). As Boebert and McCollum teach that the input/output processing unit and the access monitor unit operate within a secure computer, one of ordinary skill would recognize that tampering with the input/output processing unit or the access monitor unit is tampering with the secure computer and its associated file system. Further, as Boebert and McCollum teach that access to files is inhibited where the "modes and manners of access" are not permitted (Boebert: col. 9, lines 23-29), one of ordinary skill in the art would also recognize that where tampering is detected, particularly to the level where it raises an alarm, access to secure files would be inhibited in order to protect the files from any potential unauthorized access until the alarm was resolved.

Therefore, it would be obvious to modify the modified system of Boebert and McCollum with the teaching of Dryer to provide an input/output monitor unit for monitoring that the input/output processing unit or said access monitor unit is not tampered or performs a predetermined operation, and instructing to inhibit an input/output of a file if the input/output processing unit or said access monitor unit is tampered or performs an operation different from the predetermined operation. One would be motivated to do so in order to enhance security, particularly where a high degree of confidentiality is required.

Regarding claim 13, the modified system of Boebert and McCollum is relied upon as applied to claim 1, but Boebert and McCollum do not explain a file access log processing unit for storing and managing information on each file access sent to said access control processing unit.

However, Dryer teaches a file access log processing unit (logging task 130) for storing and managing information on each file access sent to said access control processing unit (para. 0012) for the purpose of enhancing security (para. 0011).

Therefore, it would be obvious to modify the modified system of Boebert and McCollum with the teaching of Dryer to provide for a file access log processing unit for storing and managing information on each file access sent to said access control processing unit. One would be motivated to do so in order to enhance security.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.


Orita (US 5,163,147) and Gore (US 5,771,379) each disclose a computer system with file access control functionality.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John Elmore whose telephone number is 571-272-4224. The examiner can normally be reached on M 10-8, T-Th 9-7.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 571-272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

John Elmore


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100